JC10 Rec'd PCT/PTO 28 JAN 2002

FORM PTO-1390 (REV. 5-93) — U.S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER: 2345/172

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

U S. APPLICATION NO (If known, see 37 CFR 1 5): 10/049258

INTERNATIONAL APPLICATION NO	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED.
PCT/EP00/06387	06 July 2000 (06.07.00)	27 July 1999 (27.07.99)

TITLE
METHOD FOR GENERATING/REGENERATING AN ENCRYPTION KEY FOR A CRYPTOGRAPHIC METHOD

APPLICANT(S) FOR DO/EO/US
Joerg SCHWENK

Applicant(s) herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U S C 371
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U S.C 371
3. ☒ This is an express request to begin national examination procedures (35 U S C 371(f)) immediately rather than delay examination until the expiration of the applicable time limit set in 35 U S C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U S C 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U S C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau
   c. ☐ have not been made, however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U S C 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U S.C 371(c)(4)) . (UNSIGNED)
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U S C. 371(c)(5))

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording A separate cover sheet in compliance with 37 CFR 3 28 and 3 31 is included
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☒ A substitute specification and a marked up version of the substitute specification
15. ☐ A change of power of attorney and/or address letter
16. ☒ Other items or information International Search Report and Form PCT/RO/101 Provisional International Report of Examination

Express Mail No.: EL179952105US

U.S. APPLICATION NO (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
10/049258	PCT/EP00/06387	2345/172

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)):		
Search Report has been prepared by the EPO or JPO $890 00		
International preliminary examination fee paid to USPTO (37 CFR 1 482) . $710.00		
No international preliminary examination fee paid to USPTO (37 CFR 1 482) but international search fee paid to USPTO (37 CFR 1 445(a)(2)) $740 00		
Neither international preliminary examination fee (37 CFR 1 482) nor international search fee (37 CFR 1 445(a)(2)) paid to USPTO $1,040 00		
International preliminary examination fee paid to USPTO (37 CFR 1 482) and all claims satisfied provisions of PCT Article 33(2)-(4) $100 00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 890	
Surcharge of $130 00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1 492(e))	$	

Claims	Number Filed	Number Extra	Rate		
Total Claims	8 - 20 =	0	X $18 00	$0	
Independent Claims	1 - 3 =	0	X $84 00	$0	
Multiple dependent claim(s) (if applicable)			+ $280 00	$	
TOTAL OF ABOVE CALCULATIONS =				$890	
Reduction by 1/2 for filing by small entity, if applicable Verified Small Entity statement must also be filed. (Note 37 CFR 1 9, 1 27, 1 28)				$	
SUBTOTAL =				$890	
Processing fee of $130 00 for furnishing the English translation later the ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)) +				$	
TOTAL NATIONAL FEE =				$890	
Fee for recording the enclosed assignment (37 CFR 1.21(h)) The assignment must be accompanied by an appropriate cover sheet (37 CFR 3 28, 3 31). $40.00 per property +				$	
TOTAL FEES ENCLOSED =				$890	
				Amount to be refunded	$
				charged	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed

b. ☒ Please charge my Deposit Account No 11-0600 in the amount of $890 00 to cover the above fees. A duplicate copy of this sheet is enclosed

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600 A duplicate copy of this sheet is enclosed

NOTE: Where an appropriate time limit under 37 CFR 1 494 or 1 495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status

By: Reg No 35,192

SIGNATURE

SEND ALL CORRESPONDENCE TO
Kenyon & Kenyon
One Broadway
New York, New York 10004

Telephone No (212)425-7200
Facsimile No. (212)425-5288

Richard L. Mayer, Reg. No. 22,490
NAME

1/28/02
DATE

CUSTOMER NO. 26646

[2345/172]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)	:	Joerg Schwenk
Serial No.	:	To Be Assigned
Filed	:	Herewith
For	:	METHOD FOR GENERATING/REGENERATING AN ENCRYPTION KEY FOR A CRYPTOGRAPHIC METHOD
Art Unit	:	To Be Assigned
Examiner	:	To Be Assigned

Assistant Commissioner
for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT AND
37 C.F.R. § 1.125 SUBSTITUTE SPECIFICATION STATEMENT

SIR:

Please amend without prejudice the above-identified application before examination, as set forth below.

IN THE TITLE:

Please replace the title with the following:

--METHOD FOR GENERATING/REGENERATING AN ENCRYPTION KEY FOR A CRYPTOGRAPHIC METHOD--.

IN THE SPECIFICATION AND ABSTRACT:

In accordance with 37 C.F.R. § 1.121(b)(3), a Substitute Specification (including the Abstract, but without claims) accompanies this response. It is respectfully requested that the Substitute Specification (including Abstract) be entered to replace the Specification of record.

IN THE CLAIMS:

Without prejudice, please cancel original claims 1 to 8 in the original application and please add new claims 9 to 16 as follows:

9. (New) A method for at least one of generating and regenerating an encryption key for a cryptographic method, comprising:

generating a seed S, the seed S being a large random number, only on a side of a user by consulting at least one quantity u known only to the user, the encryption key C and a public key U being generated from the seed S by using at least one predefined deterministic method;

generating a regeneration information R on the side of the user to regenerate the seed S and from which the seed S may be derived deterministically by a trust center by linking only to a secret information v known to the trust center;

storing the regeneration information R so that the regeneration information R is secured against loss,

wherein if the encryption key C is unavailable then the seed S is reconstructable by the trust center by linking the regeneration information to the secret information v.

10. (New) The method of claim 9, further comprising providing a key agreement mapping k: k(x,y)=z, and wherein:

a) k(k(u,v),w) = k(k(u,w),v) for all u,v,w;

b) from the knowledge of u and k(u,v), v cannot be inferred;

c) from the knowledge of u, k(u,v) and k(u,w), k(k(u,w)v) cannot be inferred;

wherein a public parameter g known to the trust center and a secret key v available at the trust center are linked to a public key V=k(g,v) of the trust center;

wherein the public key V and the at least one quantity u selected on the user side are linked on the user side to the seed S=k(V,u);

wherein a key pair made up of an encryption key C and a public user key U is derived from seed S on the user side using the at least one predefined deterministic method; and

wherein to reconstruct the key pair of the encryption key C and the public user key U, the regeneration information R=k(g,u) is generated on the user side and is stored so as to be protected against loss.

11. (New) The method of claim 9, further comprising providing a key agreement mapping k which is a discrete exponential function modulo a large prime number p: $k(x,y) := x^y$ modulo p, and providing that a public parameter g is an element of a mathematical field GF(p) of a high multiplicative power.

12. (New) The method of claim 9, further comprising providing a key agreement mapping k which is a multiplication on an elliptic curve.

13. (New) The method of claim 9, wherein the trust center calculates the seed S=(R,v) from the regeneration information R so as to reconstruct the encryption key C.

14. (New) The method of claim 9, further comprising deriving a new public key U and a new encryption key C when the seed S is calculated, due to loss of at least one of the encryption key C and the public key U; and

verifying by the trust center whether the new public key U is identical to the prior public key U,

wherein when verified that the new public key U is identical to the prior public key U then providing a reconstructed encryption key C to the user.

15. (New) The method of claim 10, further comprising providing a plurality of trust centers which employ the key agreement mapping k and the public parameter g;

selecting at least one of the plurality of trust centers, so that each of the selected trust centers assist in generating a partial seed Sv of the seed S being generated on the side of the user and the partial seed Sv being linked on the side of the user to the seed S, in generating the encryption key C;

calculating by the selected trust centers their respective partial seed Sv of the seed S using the regeneration information R, to regenerate the encryption key C in the case of loss;

reconstructing the encryption key C by linking in combination with each other the respective reconstructed partial seed Sv of each respective selected trust center.

16. (New) The method of claim 15, wherein the trust center and the plurality of trust centers each use at least one of a respective different function kv and a respective different public

parameter gv to create a separate regeneration information Rv for each of the trust centers selected.

REMARKS

This Preliminary Amendment cancels without prejudice original claims 1 to 8 in the underlying PCT Application No. PCT/EP00/06387, and adds without prejudice new claims 9 to 16. The new claims conform the claims to U.S. Patent and Trademark Office rules and do not add new matter to the application.

In accordance with 37 C.F.R. § 1.121(b)(3), the Substitute Specification (including the Abstract, but without the claims) contains no new matter. The amendments reflected in the Substitute Specification (including Abstract) are to conform the Specification and Abstract to U.S. Patent and Trademark Office rules or to correct informalities. As required by 37 C.F.R. § 1.121(b)(3)(iii) and § 1.125(b)(2), a Marked Up Version Of The Substitute Specification comparing the Specification of record and the Substitute Specification also accompanies this Preliminary Amendment. In the Marked Up Version, double-underlining indicates added text and bracketing indicates deleted text. Approval and entry of the Substitute Specification (including Abstract) is respectfully requested.

The underlying PCT Application No. PCT/EP00/06387 includes an International Search Report, dated December 13, 2000. The Search Report includes a list of documents that were uncovered in the underlying PCT Application. A copy of the Search Report accompanies this Preliminary Amendment.

The underlying PCT Application No. PCT/EP00/06387 also includes an International Preliminary Examination Report, dated December 7, 2001. An English translation of the International Preliminary Examination Report accompanies this Preliminary Amendment.

Applicant asserts that the subject matter of the present application is new, non-obvious, and useful. Prompt consideration and allowance of the application are respectfully requested.

Respectfully Submitted,

KENYON & KENYON

By: Reg No 35,952

Dated: 1/28/02

By: _____
Richard L. Mayer
(Reg. No. 22,490)

One Broadway
New York, NY 10004
(212) 425-7200 (telephone)
(212) 425-5288 (facsimile)

CUSTOMER NO. 26646

1/prts

[2345/172]

METHOD FOR GENERATING/REGENERATING AN ENCRYPTION KEY FOR A CRYPTOGRAPHIC METHOD

The present invention is directed to a method for generating/regenerating an encryption key for a cryptographic method, the encryption key, as well as a public key being generated using a predefined deterministic method, from a large random number (seed).

It is becoming more and more popular to employ the cryptographic technique of encryption to secure communications data and stored data. In this context, the data are enciphered under the control of a cryptographic key. The data can also be deciphered again using the same key. Marketable products and software libraries are available for this purpose.

In encryption operations, a so-called hybrid method is mostly used. In this method, the actual message is encrypted using a randomly selected symmetric key (session key) and a preselected symmetric encryption method (e.g., DES, IDEA). The session key is then encrypted, in turn, in each case using the public key of the receiver (a plurality of receivers is possible) and using a predefined asymmetric or public key method (e.g., RSA, EIGamal). The session key encrypted using this process is included with the encrypted message for each receiver. A description of this procedure and of the algorithms employed is found, for example, in William Stallings: "Cryptography and Network Security: Principles and Practice", Prentice Hall, Upper Saddle River, New

Jersey, 1998.

To decode a received message, the receiver must first decipher the session key using his/her private key, which belongs to his/her public key, and a preselected public key algorithm, to then decrypt the message using this session key.

Besides encrypting messages, cryptographic methods are also used to encrypt stored data, e.g., on one's own personal computer. Here as well, one typically employs a hybrid method, where the user first encrypts the data using a randomly selected symmetric key (session key) and a predefined symmetric encryption method (e.g., DES, IDEA). The session key is then encrypted, in turn, using the user's public key and a preselected asymmetric or public key method (e.g., RSA, EIGamal).

Using his/her private key, which belongs to his/her public key, and the predefined public key algorithm, the user first encrypts the session key and then, using this session key, the stored data.

In the following, the term "encryption key" is used in each case to refer to the user's, i.e., the receiver's private key.

The encryption key is either stored on a smart card, access to the smart card being protected by a personal identification number (PIN) known only to the user, or it is stored on another storage medium (for example, a hard disk or diskette), in which case it is preferably protected by a long password.

It can happen that the encryption key is lost. For example, if the storage medium where it was located is destroyed, or if the user forgets the PIN number or the password which he/she used to secure the encryption key, then it is no longer possible to use it to access the encrypted data.

To be able to make encrypted data accessible again in the event the encryption key is lost, mechanisms are needed to enable the encryption key to be regenerated in a secure manner. For this purpose, the encryption key is typically generated nowadays at a trust center and securely stored. As a rule, the encryption key is produced by initially generating a large random number (seed) using a statistically valid random process. From this random number, the key pair made up of the public key/private key is then generated with the aid of a deterministic method. This seed is subsequently deleted. If necessary, a copy of his/her encryption key is then delivered to the user for use.

In the process, the user does not have any influence on how his/her encryption key is generated and stored. Moreover, it is expensive to transport the generated encryption key to the user in a secure manner. As a transport medium, nowadays, one uses, for example, the above-mentioned smart card, which is sent to the user. Also, one cannot rule out a misuse of the stored key by the trust center, or one's own key becoming known due to a malfunction in the described procedure at the trust center.

The object of the present invention is to provide a method of the type mentioned at the outset which will

overcome the above-mentioned disadvantages. In particular, the method intends to leave it solely up to the user to decide whether a key should be reconstructed.

The idea underlying the method proposed here to achieve the objective is that the need for storing the encryption key for security purposes at the trust center may be eliminated when the seed (S) is only generated on the user side, in that quantities (u) known only to the user are consulted; that regeneration information (R), which is suitable for regenerating the seed and from which the seed is able to be derived deterministically by the trust center by linking only to information (v) known to it, is generated on the user side and is stored so as to be secured against lost; and that, in the event of loss of encryption key (C), seed (S) is reconstructed by the trust center by linking regeneration information (R) to secret information (v).

This may be implemented in a first embodiment of the present invention in that a mathematical mapping (key agreement mapping) k:

k(x,y)=z is provided, for which it holds that:

a) k(k(u,v),w) = k(k(u,w),v) for all u,v,w;

b) from the knowledge of u and k(u,v), in practice, one cannot infer v;

c) from the knowledge of u, k(u,v) and k(u,w), in practice, one cannot infer k(k(u,w)v);

that a public parameter g known to the trust center and a secret key v available at the trust center are linked to a public key V=k(g,v) of the trust center;

that public key V and a random number u selected on the user side are linked on the user side to seed S=k(V,u);

that a key pair made up of encryption key C and public

user key U is derived from seed S on the user side using the predefined deterministic method; and
that to render possible the reconstruction of this key pair U and C, regeneration information R=k(g,u) is generated on the user side and is stored so as to be protected against loss.

Once regeneration information R is generated, random number u and seed S should again be destroyed for security reasons. Regeneration information R is generated under tap-proof conditions, for example within the user-side computer terminal, so that there is no chance of random number u or of seed S falling into the hands of the public. Without knowledge of secret key v, regeneration information R, by itself, is not suitable for deciphering messages and data and, therefore, does not need to be kept secret.

Regeneration information R may be stored at any location (for example on paper) and, when needed, be sent over any tappable route (mail, e-mail, WWW, ftp, ...) to the trust center.
Examples of suitable key agreement mappings k are known from the theory of numbers. Provision may be made, for example, for key agreement mapping k to be a discrete exponential function modulo a large prime number p: $k(x,y) := x^y$ modulo p, and for public parameter g to be an element of a mathematical field GF(p) of a high multiplicative power, or for key agreement mapping k to be the multiplication on an elliptic curve. In practice, one should select the order of magnitude of the numbers used such that, even by summoning up modern technical means, it is impossible to calculate value y from values x and k(x,y), which, presupposing today's deciphering

technology, is ensured at orders of magnitude of the prime numbers used of between 500 and 1000 bits.

A description of such functions may be found in William Stallings: "Cryptography and Network Security: Principles and Practice", Prentice Hall, Upper Saddle River, New Jersey, 1998. The present invention makes use of the Diffie-Hellman key exchange principle, which is likewise described in the mentioned work. As described above, however, the method of the present invention presupposes a trust center, which, if needed, is able to regenerate encryption key C with the aid of regeneration information R.

In a further embodiment of the present invention, to reconstruct encryption key C in the event of a loss, seed S=k(R,v) may be calculated by the trust center from regeneration information R. The lost encryption key C is, itself, able to be calculated from the thus reconstructed seed S using the deterministic method.

Due to the property of mapping k which is used, it holds that $k(R,v) = k(k(g,u),v) = k(k(g,v),u) = k(V,u) = S$, which actually corresponds, again, to original seed S. Since the deterministic method is likewise known to the trust center, using regeneration information R, the trust center is able to readily reproduce encryption key C, even without knowledge of random number u. The regenerated encryption key C must then be relayed to the user over a tap-proof channel.

To prevent the method of the present invention from being misused to obtain private encryption keys C belonging to others, provision may also be made, once seed S is

calculated and the user's new public key U and the new encryption key C are derived due to the loss of a key, for the trust center to verify whether the newly calculated public key U is identical to the user's original public key U, and for reconstructed encryption key C to only be handed over to the user when this is conclusive. A method for securely linking the user's identity to his/her public key U is known from ITU standard X.509.

Another embodiment of the method provides for there to be a plurality of trust centers which employ key agreement mapping k and public parameter g. In generating encryption key C, one or more of these trust centers is selected, with the aid of each of the selected trust centers, another fraction value Sv of the seed being generated on the user side, as described, and partial seed Sv being linked on the user side to seed S. To regenerate encryption key C in the case of loss, the selected trust centers calculate their respective fraction value Sv of seed S using regeneration information R. To reconstruct encryption key C, the reconstructed fraction values Sv are linked, in combination with one another, to seed S. The procedure can prevent a trust center from misusing the method, since each trust center is able to generate only one partial seed Sv which, by itself, is unusable.

Another embodiment of the method provides for the various trust centers to use different functions kv and/or different public parameters gv, and for separate regeneration information Rv to be created for each of the selected trust centers. In such a case, the user must implement the method of the present invention for each

trust center, and each trust center must generate its particular partial seed Sv using its specific regeneration information Rv.

Exemplary embodiments of the present invention are represented by several figures in the drawing and are elucidated in the following description. The figures show:

Figure 1 a flow chart for generating a key part specific to a user; and

Figure 2 a flow chart for reconstructing the encryption key, following a loss.

Identical or corresponding parts are provided with the same reference numerals in the figures.

Figure 1 shows a time-related flow chart of the processes required for generating a reconstructable, user-specific encryption key C and public user key U in accordance with the method of the present invention. In the column denoted by N, the user-side data occurring one after another are listed from top to bottom. Ü designates the data transmission link to a trust center V. Trust center V and user N have public parameter g and large prime number p. Public key $V = g^v$ modulo p is generated by trust center V and transmitted by simple channels to user N. In response thereto, the user, using a random number u that he/she selects, generates a seed S and regeneration information R and again erases random number u for security reasons. Regeneration information G is transmitted to trust center V. By applying a predefined deterministic method known to the user and the trust

center, a public user key U, as well as a private, likewise user-specific encryption key C is generated from seed S. Encryption key C is used here for decrypting messages or data from the user.

In the case that the encryption key is lost, the trust center, as shown in Figure 2, regenerates seed S and encryption key C from regeneration information R, transmitted by the user to the trust center, by linking to secret key v and communicates it by secure channels to the user.

What is claimed is:

1. A method for generating/regenerating an encryption key for a cryptographic method, the encryption key, as well as a public key being generated using a predefined deterministic method, from a large random number (seed),
wherein the seed (S) is only generated on the user side, in that quantities (u) known only to the user are consulted; that regeneration information (R), which is suitable for regenerating the seed and from which the seed is able to be derived deterministically by the trust center by linking only to information (v) known to it, is generated on the user side and is stored so as to be secured against lost; and that, in the event of loss of the encryption key (C), the seed (S) is reconstructed by the trust center by linking the regeneration information (R) to the secret information (v).

2. The method as recited in Claim 1,
wherein a mathematical mapping (key agreement mapping) k: k(x,y)=z is provided, for which it holds that:
   a) k(k(u,v),w) = k(k(u,w),v) for all u,v,w;
   b) from the knowledge of u and k(u,v), in practice, one cannot infer v;
   c) from the knowledge of u, k(u,v) and k(u,w), in practice, one cannot infer k(k(u,w)v);
that a public parameter g known to the trust center and a secret key v available at the trust center are linked to a public key V=k(g,v) of the trust center; that the public key V and a random number u selected on the user side are linked on the user side to the

seed S=k(V,u);
that the key pair made up of encryption key C and public user key U is derived from seed S on the user side using the predefined deterministic method; and that to render possible the reconstruction of this key pair U and C, the regeneration information R=k(g,u) is generated on the user side and is stored so as to be protected against loss.

3. The method as recited in one of the preceding claims,
wherein the key agreement mapping k is a discrete exponential function modulo a large prime number p: $k(x,y) := x^y$ modulo p, and that the public parameter g is an element of a mathematical field GF(p) of a high multiplicative power.

4. The method as recited in one of the Claims 1 or 2, wherein the key agreement mapping k is the multiplication on an elliptic curve.

5. The method as recited in one of the preceding claims,
wherein to reconstruct the encryption key C in the event of a loss, the seed S=k(R,v) is calculated by the trust center from the regeneration information R.

6. The method as recited in one of the preceding claims,
wherein, once the seed S is calculated and the user's new public key U and the new encryption key C are derived due to the loss of a key, the trust center verifies whether the newly calculated public

key U is identical to the user's original public key U, and the reconstructed encryption key C is only be handed over to the user when this is conclusive.

7. The method as recited in one of the preceding claims,
wherein there is a plurality of trust centers which employ the key agreement mapping k and the public parameter g. In generating the encryption key C, one or more of these trust centers is selected, with the aid of each of the selected trust centers, another fraction value Sv of the seed being generated on the user side, as described, and the partial seed Sv being linked on the user side to the seed S. To regenerate the encryption key C in the case of loss, the selected trust centers calculate their respective fraction value Sv of the seed S using the regeneration information R. The reconstructed fraction values Sv are linked, in combination with one another, to the seed S to reconstruct the encryption key C.

8. The method as recited in Claim 7,
wherein the various trust centers use different functions kv and/or different public parameters gv, and separate regeneration information Rv is created for each of the selected trust centers.

Abstract

In a method for generating/regenerating an encryption key for a cryptographic method, the encryption key, as well as a public key being generated using a predefined deterministic method, from a large random number (seed), the seed is only generated on the user side, in that quantities known only to the user are consulted. Regeneration information (R), which is suitable for regenerating the seed and from which the seed is able to be derived deterministically by the trust center by linking only to information known to it, is generated on the user side and is stored so as to be secured against lost. In the event of loss of the encryption key, the seed is reconstructed by the trust center by linking the regeneration information to the secret information.

[2345/172]

METHOD FOR GENERATING/REGENERATING AN ENCRYPTION KEY FOR A CRYPTOGRAPHIC METHOD

FIELD OF THE INVENTION

The present invention relates to a method for generating and/or regenerating an encryption key for a cryptographic method. Specifically, the present invention relates to providing and using the encryption key, as well as a public key being generated using a predefined deterministic method, from a large random number (seed).

BACKGROUND INFORMATION

The cryptographic technique of encryption to secure communications data and stored data appears to be employed more often. In this context, the data are enciphered (or encrypted) under the control of a cryptographic key. The data can also be deciphered again using the same key. Marketable products and software libraries may be available for this purpose.

In encryption operations, a so-called hybrid method may be used. In this method, the actual message is encrypted using a randomly selected symmetric key or session key and a preselected symmetric encryption method, e.g., Data Encryption Standard (DES) and/or International Data Encryption Algorithm(IDEA). The session key is then encrypted, in turn, in each case using the public key of the receiver (a plurality of receivers may be involved) and

using a predefined asymmetric or public key method, e.g., Rivest, Shamir, Adleman code (RSA) and/or EIGamal (a public key encryption algorithm). The session key encrypted using this process is included with the encrypted message for each receiver. The reference "Cryptography and Network Security: Principles and Practice", by William Stallings, Prentice Hall, Upper Saddle River, New Jersey, 1998, appears discuss this procedure and the algorithms employed.

To decode a received message, the receiver must first decipher the session key using his/her private key, which belongs to his/her public key, and a preselected public key algorithm, to then decrypt the message using this session key.

Besides encrypting messages, cryptographic methods may also be used to encrypt stored data, e.g., on one's own personal computer. Here as well, one may employ a hybrid method, where the user first encrypts the data using a randomly selected symmetric key or session key and a predefined symmetric encryption method, e.g., DES and/or IDEA. The session key is then encrypted, in turn, using the user's public key and a preselected asymmetric or public key method, e.g., RSA and/or EIGamal.

Using his/her private key, which belongs to his/her public key, and the predefined public key algorithm, the user first encrypts the session key and then, using this session key, the stored data.

In the following, the term "encryption key" is used in each case to refer to the user's, i.e., the receiver's, private key.

The encryption key is either stored on a smart card, access to the smart card being protected by a personal identification number (PIN) known only to the user, or it is stored on another storage medium (for example, a hard disk or diskette), in which case it is preferably protected by a long password.

It can happen that the encryption key is lost. For example, if the storage medium where it was located is destroyed, or if the user forgets the PIN number or the password which he/she used to secure the encryption key, then it is no longer possible to use it to access the encrypted data.

To be able to make encrypted data accessible again in the event the encryption key is lost, mechanisms are needed to enable the encryption key to be regenerated in a secure manner. For this purpose, the encryption key is typically generated nowadays at a trust center or trustee or confidential, central location and securely stored. As a rule, the encryption key is produced by initially generating a large random number (seed) using a statistically valid random process. From this random number, the key pair made up of the public key/private key is then generated with the aid of a deterministic method. This seed is subsequently deleted. If necessary, a copy of his/her encryption key is then delivered to the user for use.

In the process, the user does not have any influence on how his/her encryption key is generated and stored. Moreover, it is expensive to transport the generated encryption key to the user in a secure manner. As a transport medium, nowadays, one uses, for example, the above-mentioned smart card, which is sent to the user. Further, there is a danger of misuse of the stored key by the trust center, or one's own key becoming publicly known due to a malfunction by the trust center and/or in the procedure.

SUMMARY OF THE INVENTION

Exemplary embodiments of the present invention are directed to providing a method of the type mentioned at the outset which may leave it solely up to the user to decide whether an encryption key should be reconstructed.

Exemplary embodiments of the present invention are further directed to eliminating a need for storing the encryption key for security purposes at the trust center by effecting that when the seed (S) is only generated on the user side, in that quantities (u) known only to the user are consulted; that regeneration information (R), which is suitable for regenerating the seed and from which the seed is able to be derived deterministically by the trust center by linking only to (or concatenating or combining with) information (v) known to it, is generated on the user side and is stored so as to be secured against lost; and that, in the event of loss of encryption key (C), seed (S) is reconstructed by the trust center by linking regeneration information (R) to secret information (v).

This may be implemented in exemplary embodiments of the present invention in that a mathematical mapping (key agreement mapping) k:

k(x,y)=z is provided, for which it holds that:

a) k(k(u,v),w) = k(k(u,w),v) for all u,v,w;

b) from the knowledge of u and k(u,v), in practice, one cannot infer v;

c) from the knowledge of u, k(u,v) and k(u,w), in practice, one cannot infer k(k(u,w)v);

that a public parameter g known to the trust center and a secret key v available at the trust center are linked to a public key V=k(g,v) of the trust center;

that public key V and a random number u selected on the user side are linked on the user side to seed S=k(V,u);

that a key pair made up of encryption key C and public user key U is derived from seed S on the user side using the predefined deterministic method; and

that to render possible the reconstruction of this key pair U and C, regeneration information R=k(g,u) is generated on the user side and is stored so as to be protected against loss.

In a further exemplary embodiment of the present invention, once regeneration information R is generated, random number u and seed S should again be destroyed for security reasons. Regeneration information R may be generated under tap-proof conditions, for example, within the user-side computer terminal, so that there is no chance of random number u or of seed S falling into the hands of the public. Without knowledge of secret key v, regeneration information R, by

itself, may not be suitable for deciphering messages and data and, therefore, does not need to be kept secret.

Regeneration information R may be stored at any location, for example, on paper, and then when needed be sent or transmitted over any tappable route, for example, mail, e-mail, www or internet, ftp, etc., to the trust center.

Examples of suitable key agreement mappings k include those available from the theory of numbers. Provision may be made, for example, for key agreement mapping k to be a discrete exponential function modulo a large prime number p: $k(x,y) := x^y$ modulo p, and for public parameter g to be an element of a mathematical field GF(p) of a high multiplicative power, or for key agreement mapping k to be the multiplication on an elliptic curve. In practice, in a further exemplary embodiment of the present invention, one should select the order of magnitude of the numbers used such that, even by summoning up modern technical means, it may be impossible to calculate value y from values x and k(x,y), which, presupposing today's deciphering technology, is ensured at orders of magnitude of the prime numbers used of between 500 and 1000 bits.

The reference "Cryptography and Network Security: Principles and Practice", by William Stallings, Prentice Hall, Upper Saddle River, New Jersey, 1998, appears to discuss such formulations, including the Diffie-Hellman key exchange principle.

The present invention makes use of the Diffie-Hellman key exchange principle. Exemplary embodiments of the method of the present invention presupposes a trust center, which, if needed, is able to regenerate encryption key C with the aid of regeneration information R.

In further exemplary embodiments of the present invention, to reconstruct encryption key C in the event of a loss, seed S=k(R,v) may be calculated by the trust center from regeneration information R. The lost encryption key C is, itself, able to be calculated from the thus reconstructed seed S using the deterministic method.

Due to the property of mapping k which is used, it holds that k(R,v) = k(k(g,u),v) = k(k(g,v),u) = k(V,u) = S, which actually corresponds, again, to original seed S. Since the deterministic method may be available to be known to the trust center, using regeneration information R, the trust center can be able to readily reproduce encryption key C, even without knowledge of random number u. The regenerated encryption key C should then be relayed to the user over a tap-proof channel or route.

In a further exemplary embodiment of the present invention, to prevent the method of the present invention from being misused to obtain private encryption keys C belonging to others, provision may also be made, once seed S is calculated and the user's new public key U and the new encryption key C are derived due to the loss of a key, for the trust center to verify whether the newly calculated

public key U is identical to the user's original public key U, and for reconstructed encryption key C to only be handed over to the user when this verification is conclusive. A method for securely linking the user's identity to his/her public key U is available by ITU standard X.509.

A further exemplary embodiment of the present invention is directed to providing for there to be a plurality of trust centers which employ key agreement mapping k and public parameter g. In generating encryption key C, one or more of these trust centers may be selected, with the aid of each of the selected trust centers, another fraction value Sv of the seed being generated on the user side, as described, and partial seed Sv being linked on the user side to seed S. To regenerate encryption key C in the case of loss, the selected trust centers may calculate their respective fraction value Sv of seed S using regeneration information R. To reconstruct encryption key C, the reconstructed fraction values Sv are linked, in combination with one another, to seed S. The procedure can prevent a trust center from misusing the method, since each trust center is able to generate only one partial seed Sv which, by itself, is unusable.

A further embodiment of the present invention is directed to providing for the various trust centers to use different functions kv and/or different public parameters gv, and for separate regeneration information Rv to be created for each of the selected trust centers. In such a case, the user must implement the method of the present invention for each trust

center, and each trust center must generate its particular partial seed Sv using its specific regeneration information Rv.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a flow chart for generating a key part specific to a user.

Figure 2 shows a flow chart for reconstructing the encryption key, following a loss.

DETAILED DESCRIPTION

Figure 1 shows a time-related flow chart of the processes required for generating a reconstructable, user-specific encryption key C and public user key U in accordance with the method of the present invention. In the column denoted by N, the user-side data occurring one after another are listed from top to bottom. U designates the data transmission link to a trust center V. Trust center V and user N have public parameter g and large prime number p. Public key $V = g^v$ modulo p is generated by trust center V and transmitted by simple channels or means to user N. In response thereto, the user, using a random number u that he/she selects, generates a seed S and regeneration information R and again erases random number u for security reasons. Regeneration information G is transmitted to trust center V. By applying a predefined deterministic method known to the user and the trust center, a public user key U, as well as a private, likewise user-specific encryption key C is generated from seed S. Encryption key C is used here

for decrypting messages or data from the user.

In the case that the encryption key is lost, the trust center, as shown in Figure 2, regenerates seed S and encryption key C from regeneration information R, transmitted by the user to the trust center, by linking to secret key v and communicates it by secure channels or other such means to the user.

WHAT IS CLAIMED IS:

ABSTRACT OF THE DISCLOSURE

A method for generating/regenerating an encryption key for a cryptographic method including the encryption key as well as a public key being generated using a predefined deterministic method from a large random number (seed), where the seed is only generated on the user side, and for which quantities available only to the user are consulted. Regeneration information (R), which is suitable for regenerating the seed and from which the seed is able to be derived deterministically by the trust center by linking only to information known to it, may be generated on the user side and stored so as to be secured against lost. In the event of loss of the encryption key, the seed may be reconstructed by the trust center by linking the regeneration information to the secret information.

[redacted]

[2345/172]

METHOD FOR GENERATING/REGENERATING AN ENCRYPTION KEY FOR A CRYPTOGRAPHIC METHOD

FIELD OF THE INVENTION

The present invention [is directed] relates to a method for [generating/regenerating] generating and/or regenerating an encryption key for a cryptographic method. Specifically, the present invention relates to providing and using the encryption key, as well as a public key being generated using a predefined deterministic method, from a large random number (seed).

[It is becoming more and more popular to employ

BACKGROUND INFORMATION

The cryptographic technique of encryption to secure communications data and stored data appears to be employed more often. In this context, the data are enciphered (or encrypted) under the control of a cryptographic key. The data can also be deciphered again using the same key. Marketable products and software libraries [are] may be available for this purpose.

In encryption operations, a so-called hybrid method [is usually] may be used. In this method, the actual message is encrypted using a randomly selected symmetric key [(]or session key[)] and a preselected symmetric encryption method [(e.g., DES, IDEA)], e.g., Data Encryption Standard (DES) and/or International Data Encryption Algorithm(IDEA). The session key is then encrypted, in turn, in each case

using the public key of the receiver (a plurality of receivers may be involved) and using a predefined asymmetric or public key method, e.g., Rivest, Shamir, Adleman code (RSA) and/or EIGamal (a public key encryption algorithm). The session key encrypted using this process is included with the encrypted message for each receiver. The reference "Cryptography and Network Security: Principles and Practice", by William Stallings, Prentice Hall, Upper Saddle River, New Jersey, 1998, discuss this procedure and the algorithms employed.

To decode a received message, the receiver must first decipher the session key using his/her private key, which belongs to his/her public key, and a preselected public key algorithm, to then decrypt the message using this session key.

Besides encrypting messages, cryptographic methods may also be used to encrypt stored data, e.g., on one's own personal computer. Here as well, one may employ a hybrid method, where the user first encrypts the data using a randomly selected symmetric key or session key and a predefined symmetric encryption method, e.g., DES, and/or IDEA. The session key is then encrypted, in turn, using the user's public key and a preselected asymmetric or public key method, e.g., RSA, and/or EIGamal.

Using his/her private key, which belongs to his/her public key, and the predefined public key algorithm, the user first

encrypts the session key and then, using this session key, the stored data.

In the following, the term "encryption key" is used in each case to refer to the user's, i.e., the receiver's, private key.

The encryption key is either stored on a smart card, access to the smart card being protected by a personal identification number (PIN) known only to the user, or it is stored on another storage medium (for example, a hard disk or diskette), in which case it is preferably protected by a long password.

It can happen that the encryption key is lost. For example, if the storage medium where it was located is destroyed, or if the user forgets the PIN number or the password which he/she used to secure the encryption key, then it is no longer possible to use it to access the encrypted data.

To be able to make encrypted data accessible again in the event the encryption key is lost, mechanisms are needed to enable the encryption key to be regenerated in a secure manner. For this purpose, the encryption key is typically generated nowadays at a trust center or trustee or confidential, central location and securely stored. As a rule, the encryption key is produced by initially generating a large random number (seed) using a statistically valid random process. From this random number, the key pair made up of the public key/private key is then generated with the aid of a deterministic method. This seed is subsequently deleted. If necessary, a copy of his/her encryption key is

then delivered to the user for use.

In the process, the user does not have any influence on how his/her encryption key is generated and stored. Moreover, it is expensive to transport the generated encryption key to the user in a secure manner. As a transport medium, nowadays, one uses, for example, the above-mentioned smart card, which is sent to the user. Also, [Further,] there is a danger of misuse of the stored key by the trust center, or one's own key becoming publicly known due to a malfunction [in the described procedure of] by the trust center and/or in the procedure.

[The object] SUMMARY OF THE INVENTION

Exemplary embodiments of the present invention [is] are directed to [providing] providing a method of the type mentioned at the outset which [will overcome the above-mentioned disadvantages. In particular, the method] may leave it solely up to the user to decide whether [an] an encryption key should be reconstructed.

[The idea underlying the method proposed here to achieve the objective is that the] Exemplary embodiments of the present invention are further directed to eliminating a need for storing the encryption key for security purposes at the trust center [may be eliminated] by effecting that when the seed (S) is only generated on the user side, in that quantities (u) known only to the user are consulted; that regeneration information (R), which is suitable for regenerating the seed and from which the seed is able to be derived deterministically by the trust center by linking only to (or concatenating or combining with) information (v)

known to it, is generated on the user side and is stored so as to be secured against lost; and that, in the event of loss of encryption key (C), seed (S) is reconstructed by the trust center by linking regeneration information (R) to secret information (v).

This may be implemented in a first exemplary embodiments of the present invention in that a mathematical mapping (key agreement mapping) k:

k(x,y)=z is provided, for which it holds that:

a) k(k(u,v),w) = k(k(u,w),v) for all u,v,w;

b) from the knowledge of u and k(u,v), in practice, one cannot infer v;

c) from the knowledge of u, k(u,v) and k(u,w), in practice, one cannot infer k(k(u,w)v);

that a public parameter g known to the trust center and a secret key v available at the trust center are linked to a public key V=k(g,v) of the trust center;

that public key V and a random number u selected on the user side are linked on the user side to seed S=k(V,u);

that a key pair made up of encryption key C and public user key U is derived from seed S on the user side using the predefined deterministic method; and

that to render possible the reconstruction of this key pair U and C, regeneration information R=k(g,u) is generated on the user side and is stored so as to be protected against loss.

In a further exemplary embodiment of the present invention, once regeneration information R is generated, random number u and seed S should again be destroyed for security reasons. Regeneration information R may be

generated under tap-proof conditions, for example, within the user-side computer terminal, so that there is no chance of random number u or of seed S falling into the hands of the public. Without knowledge of secret key v, regeneration information R, by itself, may not be suitable for deciphering messages and data and, therefore, does not need to be kept secret.

Regeneration information R may be stored at any location, for example, on paper, and then when needed, be sent or transmitted over any tappable route, for example, mail, e-mail, www or internet, ftp, etc., to the trust center.

Examples of suitable key agreement mappings k include those available from the theory of numbers. Provision may be made, for example, for key agreement mapping k to be a discrete exponential function modulo a large prime number p: $k(x,y) := x^y$ modulo p, and for public parameter g to be an element of a mathematical field GF(p) of a high multiplicative power, or for key agreement mapping k to be the multiplication on an elliptic curve. In practice, in a further exemplary embodiment of the present invention, one should select the order of magnitude of the numbers used such that, even by summoning up modern technical means, it may be impossible to calculate value y from values x and k(x,y), which, presupposing today's deciphering technology, is ensured at orders of magnitude of the prime numbers used of between 500 and 1000 bits.

A description of such functions may be found in the literature. The reference "Cryptography and Network Security:

Principles and Practice", by William Stallings, Prentice Hall, Upper Saddle River, New Jersey, 1998, appears to discuss such formulations, including the Diffie-Hellman key exchange principle.

The present invention makes use of the Diffie-Hellman key exchange principle, [illegible] mentioned above, however, . Exemplary embodiments of the method of the present invention presupposes a trust center, which, if needed, is able to regenerate encryption key C with the aid of regeneration information R.

In [illegible] further exemplary embodiments of the present invention, to reconstruct encryption key C in the event of a loss, seed S=k(R,v) may be calculated by the trust center from regeneration information R. The lost encryption key C is, itself, able to be calculated from the thus reconstructed seed S using the deterministic method.

Due to the property of mapping k which is used, it holds that k(R,v) = k(k(g,u),v) = k(k(g,v),u) = k(V,u) = S, which actually corresponds, again, to original seed S. Since the deterministic method [illegible] may be available to be known to the trust center, using regeneration information R, the trust center [illegible] can be able to readily reproduce encryption key C, even without knowledge of random number u. The regenerated encryption key C [illegible] should then be relayed to the user over a tap-proof channel or route.

[illegible] In a further exemplary embodiment of the present invention, to prevent the method of the present invention

from being misused to obtain private encryption keys C belonging to others, provision may also be made, once seed S is calculated and the user's new public key U and the new encryption key C are derived due to the loss of a key, for the trust center to verify whether the newly calculated public key U is identical to the user's original public key U, and for reconstructed encryption key C to only be handed over to the user when this verification is conclusive. A method for securely linking the user's identity to his/her public key U is known from available by ITU standard X.509.

A further exemplary embodiment of the present invention is directed to providing for there to be a plurality of trust centers which employ key agreement mapping k and public parameter g. In generating encryption key C, one or more of these trust centers may be selected, with the aid of each of the selected trust centers, another fraction value Sv of the seed being generated on the user side, as described, and partial seed Sv being linked on the user side to seed S. To regenerate encryption key C in the case of loss, the selected trust centers may calculate their respective fraction value Sv of seed S using regeneration information R. To reconstruct encryption key C, the reconstructed fraction values Sv are linked, in combination with one another, to seed S. The procedure can prevent a trust center from misusing the method, since each trust center is able to generate only one partial seed Sv which, by itself, is unusable.

A further embodiment of the method provides present invention is directed to providing for the various trust centers to use different functions kv and/or

different public parameters gv, and for separate regeneration information Rv to be created for each of the selected trust centers. In such a case, the user must implement the method of the present invention for each trust center, and each trust center must generate its particular partial seed Sv using its specific regeneration information Rv.

Exemplary embodiments of the present invention are represented by several figures in the drawing and are explained in the following description. The figures show:

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a flow chart for generating a key part specific to a user; and

Figure 2 shows a flow chart for reconstructing the encryption key, following a loss.

Identical or corresponding parts are provided with the same reference numerals in the figures.

DETAILED DESCRIPTION

Figure 1 shows a time-related flow chart of the processes required for generating a reconstructable, user-specific encryption key C and public user key U in accordance with the method of the present invention. In the column denoted by N, the user-side data occurring one after another are listed from top to bottom. Ü designates the data transmission link to a trust center V. Trust center V and user N have public parameter g and large prime number p. Public key $V = g^v$ modulo p is generated by trust center V and transmitted by simple channels or means to user N. In

response thereto, the user, using a random number u that he/she selects, generates a seed S and regeneration information R and again erases random number u for security reasons. Regeneration information G is transmitted to trust center V. By applying a predefined deterministic method known to the user and the trust center, a public user key U, as well as a private, likewise user-specific encryption key C is generated from seed S. Encryption key C is used here for decrypting messages or data from the user.

In the case that the encryption key is lost, the trust center, as shown in Figure 2, regenerates seed S and encryption key C from regeneration information R, transmitted by the user to the trust center, by linking to secret key v and communicates it by secure channels or other such means to the user.

WHAT IS CLAIMED IS:

ABSTRACT OF THE DISCLOSURE

A method for generating/regenerating an encryption key for a cryptographic method, including the encryption key, as well as a public key being generated using a predefined deterministic method, from a large random number (seed), where the seed is only generated on the user side, [illegible] and for which quantities [illegible] available only to the user are consulted. Regeneration information (R), which is suitable for regenerating the seed and from which the seed is able to be derived deterministically by the trust center by linking only to information known to it, [illegible] may be generated on the user side and [illegible] stored so as to be secured against lost. In the event of loss of the encryption key, the seed [illegible] may be reconstructed by the trust center by linking the regeneration information to the secret information.

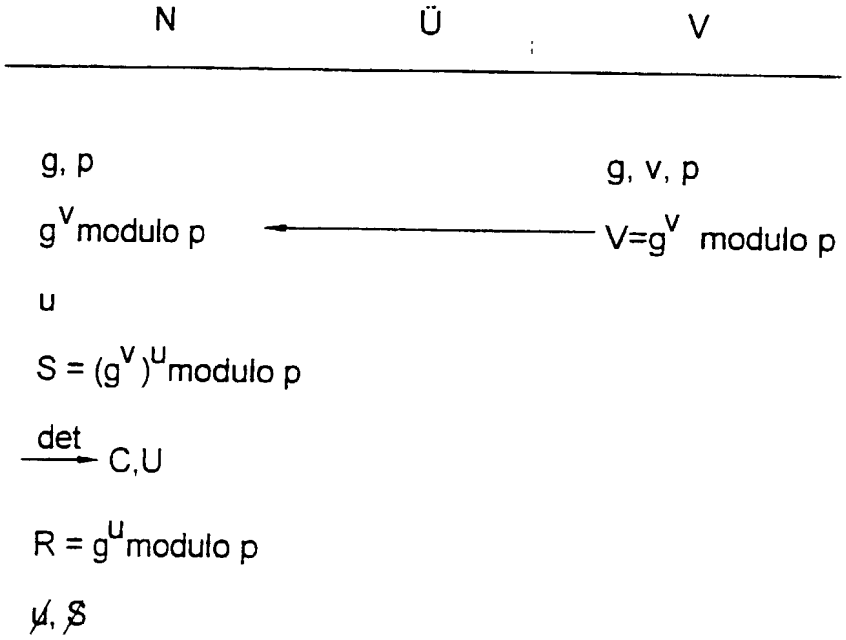
N
Ü
V
g, p
g, v, p
g^V modulo p
$V=g^V$ modulo p
u
$S = (g^V)^U$ modulo p
det
C,U
$R = g^U$ modulo p
μ, S

Fig. 1

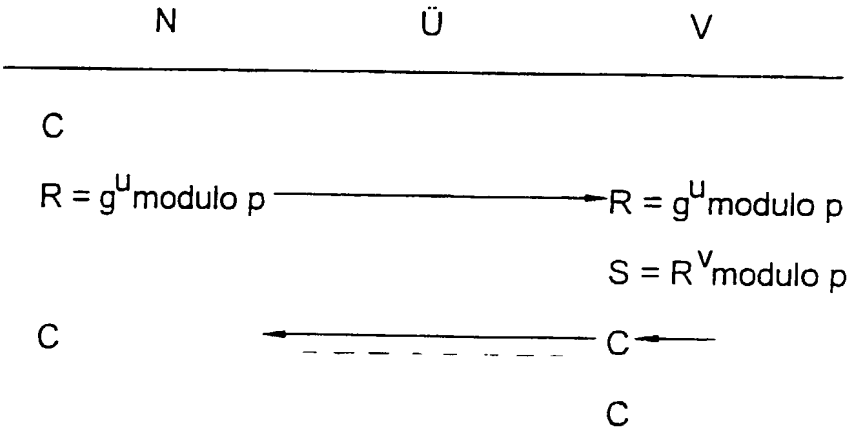
N
Ü
V
C
$R = g^U$ modulo p
$R = g^U$ modulo p
$S = R^V$ modulo p
C
C
C

Fig. 2

P99075US

2345/172

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **METHOD FOR GENERATING/REGENERATING AN ENCRYPTION KEY FOR A CRYPTOGRAPHIC METHOD** the specification of which was filed as International Application No. PCT/EP00/06387 on July 6, 2000 and filed herewith as U.S. application for Letters Patent in the U.S. Patent and Trademark Office.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

Number	Country Filed	Day/Month/Year	Priority Claimed Under 35 USC 119
199 35 285	Fed. Rep. of Germany	July 27, 1999	Yes

And I hereby appoint Richard L. Mayer (Reg. No. 22,490), Gerard A. Messina (Reg. No. 35,952) and Linda M. Shudy (Reg. No. 47,084) my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Please address all communications regarding this application to:

KENYON & KENYON
One Broadway
New York, New York 10004

CUSTOMER NO. 26646

Please direct all telephone calls to Richard L. Mayer at (212) 425-7200.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the application or any patent issued thereon.

1-00

Inventor: **Joerg SCHWENK**

Inventor's Signature: _____

Date: 1.28.02

Residence: Suedwestring 27
D-64807 Dieburg
Federal Republic of Germany

Citizenship: German

Office Address: Same as above.